

ICT
Informatiebeveiligingsplan <20XX>
voor
<stelsel, applicatie, dienst(verlening)>

Opdrachtnemer/Uitvoerder	
Naam	
Functie	
Datum	
Status	
Classificatie	Vertrouwelijk (<i>na invulling door ON</i>)
Paraaf	

Colofon

Uitgegeven door	Security Centre, Rijkswaterstaat
Informatie	
Opmaak	
Datum	12 augustus 2019
Versienummer	1.1

Inhoud

1. Inleiding	5
1.1 Algemeen.....	5
1.2 Doel	5
1.3 Scope	5
1.4 Doelgroep	5
2. Informatiebeveiligingsrisico's en eisen	6
2.1 Risico's	6
2.2 Eisen gebaseerd op de overheidsbaseline	6
3. Informatiebeveiliging beheersmaatregelen	7
3.1 Verantwoording	7
3.1.1 Comply or explain	7
3.1.2 Risico's	7
3.2 Beheersmaatregelen.....	7
3.3 Informatiebeveiligingsbeleid	8
3.3.1 Belegging verantwoordelijkheden	8
3.3.2 Borging Informatiebeveiliging	8
3.3.3 Onderaannemers	8
3.3.4 Beheer bedrijfsmiddelen en CMDB	9
3.3.5 Aanvaardbaar gebruik toegangsmiddelen verstrekt door Opdrachtgever	9
3.3.6 Classificatie, beveiliging en opslaglocatie van informatie	9
3.3.7 Bewustwording, scholing en VOG	9
3.3.8 Fysieke toegang tot werk en technische ruimten en de logische toegang tot informatiesystemen.....	10
3.3.9 Wachtwoordrichtlijn	11
3.3.10 Back-up en recovery proces	11
3.3.11 Beveiliging documentatie technisch beheer en broncode	11
3.3.12 Wijzigingsproces, aanpassingen, doorvoeren patches en testen 11	11
3.3.13 Beveiliging tegen malware, hardening en patching	12
3.3.14 Koppeling van apparatuur	13
3.3.15 Logging en monitoring	13
3.3.16 Datanetwerkkoppelingen	13
3.3.17 Remote Access en gebruik veilige datanetwerkverbindingen en communicatieprotocollen	14
3.3.18 (Web-) applicaties en mobiele apps	14
3.3.19 Continuïteit en herstel dienstverlening	15
3.3.20 Testen continuïteitsplannen	15
3.3.21 Beveiliging Spionage.....	15
3.3.22 Beveiliging van de Informatievoorziening en informatie op mobiele apparatuur	16
3.3.23 Cryptografie	16
4. Security incidenten, verhoogde dreiging en response	17
5. Informatiebeveiliging audit.....	18
5.1 Bevindingen	18
5.2 Risico's van de bevindingen	18
5.3 Aanbevelingen en verbetermaatregelen	18
6. Evaluatie beveiligingsincidenten en rapportage	19
6.1 Beveiligingsincidenten	19

6.2	Risico's van beveiligingsincidenten	19
6.3	Aanbevelingen en verbetermaatregelen	19
7.	Evaluatie security gerelateerde wijzigingen	20
7.1	Security gerelateerde wijzigingen.....	20
7.2	Overzicht security gerelateerde wijzigingen	20
7.3	Analyse security gerelateerde wijzigingen en aanbevelingen	20
8.	Evaluatie en actualisatie van risico's en beheersmaatregelen	21
8.1	Risicoanalyse en risicoafweging.....	21
8.2	Testresultaten back-up en recovery proces en continuïteitsplannen en voorzieningen	21
8.3	Informatiebeveiliging beheersmaatregelen	21
8.4	Periodieke rapportage controle accounts en autorisatie	21
8.5	Periodieke rapportage pentesten en kwetsbaarheidscans	21
8.6	Periodieke rapportage updates patches	21
8.7	Periodieke rapportage statussen explains	21
9.	Verklaring Opdrachtnemer	22
9.1	Certificering	22
9.2	Risicoanalyse en risicoafweging.....	22
10.	Bijlagen.....	23
10.1	Relevante bijlagen.....	23
10.2	Explains	23
11.	Begrippenlijst.....	24

1. Inleiding

1.1 Algemeen

Informatiebeveiliging is er op gericht om uitval, verstoring en misbruik van ICT-systemen te voorkomen en daarmee bij te dragen aan de beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van de informatievoorziening (IV) van Rijkswaterstaat.

Voor de overheid schrijft de Baseline Informatiebeveiliging Overheid (BIO) het basisniveau voor informatiebeveiliging bij de Overheid voor. De baseline biedt een normenkader voor de beveiliging van de Informatievoorziening (IV) van het Rijk. Om aan de beveiligingsdoelstellingen te voldoen, maakt RWS een vertaling naar informatiebeveiligingseisen in het contract. Primair is het doel om verstoring, misbruik en uitval binnen de ICT te voorkomen.

In dit informatiebeveiliging splan beschrijft de Opdrachtnemer hoe aan de informatiebeveiligingseisen wordt voldaan. Ook zijn de activiteiten aangegeven die nodig zijn voor de beveiliging van de IV gedurende de beheerfase en de eventuele uitfasering. Vanuit de PDCA cyclus wordt de inhoud geactualiseerd door Opdrachtnemer.

1.2 Doel

De doelstelling van dit document is om een template voor Opdrachtnemers beschikbaar te stellen waarmee de risico's met betrekking tot Informatiebeveiliging zodanig kunnen worden beheerst dat de betrouwbaarheid (in termen van beschikbaarheid, integriteit en vertrouwelijkheid) van de systemen of dienst gedurende de looptijd van het contract wordt gewaarborgd en Informatiebeveiliging toetsbaar wordt middels de Systeemgerichte Contract Beheersing (SCB) van Opdrachtgever.

1.3 Scope

Onder de scope van het Informatiebeveiliging Beveiligingsplan vallen:

<<<<Opdrachtnemer>>>> beschrijft hier wat wel en niet onder de scope van het Informatiebeveiliging Beveiligingsplan valt.

1.4 Doelgroep

Dit document is geschreven voor de Opdrachtnemer, beheerder van systeem, applicatie of dienst(verlening) maar zal door Opdrachtgever opgevraagd en getoetst worden in het kader van de Systeemgerichte Contract Beheersing (SCB).

2. Informatiebeveiligingsrisico's en eisen

2.1 Risico's

Informatiebeveiliging is het voorkomen van gevaar of schade veroorzaakt door verstoring, uitval en misbruik van ICT van Rijkswaterstaat. De beheersing van de toegang, of het nu fysiek of digitale vorm is, vormt letterlijk en figuurlijk het sleutelbegrip voor het terugdringen van de risico's voor de informatievoorziening van Rijkswaterstaat.

De mitigatie van de volgende risico's zijn vanuit de Opdrachtgever geprioriteerd (voor zover in scope):

1. Niet geautoriseerden hebben fysieke toegang tot niet openbare, werk (kantoor), en technische ruimten;
2. Niet geautoriseerden hebben logisch toegang tot de ICT -systemen en/of data van RWS;
3. Informatie over zwakke plekken in de beveiliging en beveiligingsincidenten ontbreekt alsmede een handelingsperspectief;
4. Niet geautoriseerden hebben (via Internet of draadloze toepassingen) toegang tot het RWS datanetwerk;
5. ICT -systemen bevatten kwetsbaarheden en zijn vatbaar voor malware;
6. Het niet kunnen detecteren en analyseren van afwijkend gedrag op het datanetwerk en de zich voorgedane incidenten via logging en monitoring;
7. Risico's geïntroduceerd door programmeurs, beheerders en of onderhoudsmedewerkers. Deze zijn zich niet bewust van onveilige situaties, beschikken niet over de juiste opleiding en training, hebben geen geheimhoudingsverklaring getekend of beschikken niet over een recente verklaring omtrent het gedrag;
8. Functionele wijzigingen brengen onvoorziene veiligheid- en beveiligingseffecten met zich mee en kunnen zelfs de ICT -systemen deels of volledig doen uitvallen;
9. De handhaving en de effectiviteit van de Informatiebeveiliging maatregelen is niet gewaarborgd alsmede de structurele borging bij onderaannemers;
10. Bij systeemstoringen of functionele wijzigingen is er geen terugvaloptie (geen back-up en recovery proces).

2.2 Eisen gebaseerd op de overheidsbaseline

De beveiligingsdoelstellingen en controls, die volgen uit de overheidsbaseline (de eerder genoemde BIO), zijn in het contract opgenomen. Deze vormen in relatie tot de scope van de opdracht en de geprioriteerde risico's door Opdrachtgever samen de basis van de door <<<< Opdrachtnemer>>>> uitgevoerde risicoanalyse en risicoafweging en worden nader uitgewerkt in de navolgende hoofdstukken.

3. Informatiebeveiliging beheersmaatregelen

3.1 Verantwoording

3.1.1 *Comply or explain*

<<<<Opdrachtnemer>>>> motiveert in deze paragraaf welke Informatiebeveiliging eisen uit het contract/overeenkomst niet van toepassing zijn. Ook worden in deze paragraaf afwijkende invullingen of het tijdelijk niet kunnen invullen van de informatiebeveiligingseisen beschreven in relatie tot de scope van het Informatiebeveiliging splan, zoals beschreven in paragraaf 1.3 voor het betreffende systeem, de (web-)_applicatie of dienst(verlening). Bij een afwijkende of niet tijdelijke invulling van een informatiebeveiligingseis wordt een explain opgesteld, die wordt toegevoegd in de bijlage bij dit Informatiebeveiliging beveiligingsplan. Geef bij de explain aan welke verbeterplannen hieraan gekoppeld zijn.

Een explain-verklaring bevat:

- De eis waaraan niet wordt voldaan. Voldoende begrijpelijk geformuleerd en reden waarom nog niet kan worden voldaan
- Risico van de explain
 - Voor de Opdrachtgever
 - Voor andere organisaties (+ verklaring welke organisaties)
 - Welke compenserende maatregelen getroffen worden
 - Beschrijving van het restrisico
- Reden van acceptatie van de explain
- Geldigheid (duurzaam of tijdelijk met vermelding van einddatum)
- Verantwoordelijke organisatie, actiehouder (=contactpersoon) en lijnmanager
- Refrentienummer en datum van de explain
- Status (kan tussentijds worden bijgehouden)
- Een verwijzing naar een verbeterplan.

VSP 18.2.SC-22 De Opdrachtnemer dient conform de gemaakte afspraken met Opdrachtgever inzake eventuele explains invulling te geven aan het verbeterplan voor de explains en periodiek hierover de status te rapporteren aan Opdrachtgever.

3.1.2 *Risico's*

<<<<Opdrachtnemer>>>> beschrijft hier de risico's die naar voren komen uit de initieel door Opdrachtnemer uit te voeren risicoanalyse en risicoafweging zoals vereist in de overeenkomst. De Opdrachtnemer dient voor dit systeem, (web-)applicatie, mobile app of dienst(verlening) minimaal de door Opdrachtgever in paragraaf 2.1 aangegeven risico's te mitigeren.

Indien de door Opdrachtgever aangegeven risico's niet van toepassing zijn voor het betreffende systeem, (web-)applicatie, mobile app of dienst(verlening), dan dient dit gemotiveerd te worden bij paragraaf 3.1.1 waar de 'comply or explain' regel geldt en aangegeven dat het risico niet aan de orde is binnen de scope.

VSP 12.6.1 Opdrachtnemer dient voor informatiebeveiliging minimaal jaarlijks een risicoanalyse en risicoafweging conform NEN-ISO/IEC 27005 of gelijkwaardig te maken en passende maatregelen te treffen.

3.2 Beheersmaatregelen

<<<<Opdrachtnemer>>>> heeft voor dit systeem, (web-)applicatie, mobile app en/of dienst(verlening) de hierna volgende Informatiebeveiliging beheersmaatregelen getroffen die jaarlijks worden geëvalueerd en indien nodig aangepast.

VSP 5.1.SC-01b Opdrachtnemer dient, daar waar Opdrachtgever niet verwijst naar specifieke beveiligingsrichtlijnen bij de te treffen maatregelen, de richtlijnen uit de meest recente versie van de NEN-ISO/IEC 27002 norm aan te houden.

3.3 Informatiebeveiligingsbeleid

<<<<Opdrachtnemer>>>> voegt het afschrift van zijn ISO 27001 certificering toe aan de bijlagen, samen met de van toepassing zijnde statement of applicability of Opdrachtnemer beschrijft op welke wijze zijn informatievoorziening is beveiligd en verwijst naar paragraaf 3.3.22 voor de beveiliging tegen verlies, ongeautoriseerde kennisname of wijziging van geclassificeerde informatie en documenten bij verwerking in de kantoor- en netwerkomgeving van Opdrachtnemer.

- VSP 5.1.1 Opdrachtnemer is aantoonbaar voor de overeengekomen Prestatie gecertificeerd conform de meest recente versie van de NEN-ISO/IEC 27001 norm of gelijkwaardig, en blijft dit voor ten minste de duur van de Overeenkomst.
- VSP 5.1-SC-01a Opdrachtnemer dient het deel van zijn informatievoorziening dat benodigd is voor de door de Opdrachtgever gevraagde registraties en bestanden en dat benodigd is bij de verwerking van de door de Opdrachtgever geclassificeerde informatie en Documenten, te beveiligen zodanig dat deze zijn beschermd tegen verlies, ongeautoriseerde kennisname en ongeautoriseerde wijziging.

3.3.1 Belegging verantwoordelijkheden

Bij <<<<Opdrachtnemer>>>> is de verantwoordelijkheid voor Informatiebeveiliging belegd bij de <<<<afdeling/onderdeel>>>> en is <<<<de persoon>>>> voor Opdrachtgever het eerste aanspreekpunt voor Informatiebeveiliging aangelegenheden. Bij afwezigheid zijn de vervangers bekend.

- VSP 6.1.1 Opdrachtnemer dient voor ten minste alle processen genoemd in de Overeenkomst aantoonbaar de verantwoordelijkheden, taken en bevoegdheden op de daartoe geëigende plaatsen binnen de (project)organisatie te beleggen.
- VSP 7.3.1 Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het definiëren van verantwoordelijkheden en taken met betrekking tot informatiebeveiliging voor de Prestatie en dient naar het Personeel te communiceren dat:
 1. deze van kracht blijven na beëindiging of wijziging van het dienstverband;
 2. deze ten uitvoer moeten worden gebracht.

3.3.2 Borging Informatiebeveiliging

De <<<<Opdrachtnemer>>>> beschrijft hoe de cybersecurity beheersmaatregelen in zijn managementsysteem zijn geborgd.

- VSP 6.1.5 Opdrachtnemer dient te beschikken over een operationeel geborgd projectbeheerproces voor de Prestatie waarin informatiebeveiliging aantoonbaar geïntegreerd is.
- VSP 13.1.2 Opdrachtnemer dient beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle diensten betrokken bij de Prestatie opgenomen te hebben in een Service Level Agreement (SLA) met Opdrachtgever met ten minste aandacht voor de beveiligingsaspecten beschikbaarheid, melden van incidenten, doorvoeren van wijzigingen en escalatie.
- VSP 18.2-SC-08 Opdrachtnemer dient zich te houden aan de afspraken en procedures op het gebied van informatiebeveiliging waarin doel, wijze, en frequentie van contact over de informatiebeveiliging beschreven staat op strategisch, tactisch en operationeel niveau.

3.3.3 Onderaannemers

<<<<Opdrachtnemer>>>> beschrijft op welke wijze de contracteisen geborgd zijn bij gebruik van onderaannemers die in aanraking komen met de getroffen Informatiebeveiliging beheersmaatregelen of het beheer en onderhoud van de Informatiebeveiliging maatregelen verzorgen.

- VSP 15.1.3 De Opdrachtnemer dient te borgen dat, in het geval dat voor de levering van de Prestatie gebruik wordt gemaakt van onderaannemers, bij de inkoop van diensten of producten van bedrijven de beveiligingseisen van Opdrachtgever door betrokkenen worden aangehouden.
- VSP 15.1-SC-25 De Opdrachtnemer dient, in het geval dat voor de levering van de Prestatie gebruik wordt gemaakt van onderaannemers, waarbij bij inkoop van diensten of producten vendorlock-in van een onderaannemer kan ontstaan en/of de nationale veiligheid in het geding kan worden gebracht, dit eerst voor te leggen aan Opdrachtgever.

3.3.4 Beheer bedrijfsmiddelen en CMDB

<<<<Opdrachtnemer>>>> beschrijft conform ITIL op welke wijze de Configuration Items van alle ICT worden geregistreerd in een CMDB en hoe de actualiteit van deze wordt gewaarborgd. Ook dient beschreven te worden op welke wijze deze informatie aan Opdrachtgever beschikbaar wordt gesteld.

- VSP 8.1.1a Opdrachtnemer dient aantoonbaar operationeel geborgd te hebben dat van alle informatiesystemen betrokken bij de Prestatie een inventaris is opgesteld in een Configuration Management Database (CMDB), zodanig dat deze effectief kan worden gebruikt voor een effectief Configuration Management (CM) ITIL proces en dat deze CMDB actueel wordt gehouden.
- VSP 8.1.1b Opdrachtnemer dient op verzoek van Opdrachtgever de gegevens vermeld in de Configuration Management Database (CMDB), van alle informatiesystemen betrokken bij de Prestatie, over te dragen.

3.3.5 Aanvaardbaar gebruik toegangsmiddelen verstrekt door Opdrachtgever

<<<<Opdrachtnemer>>>> beschrijft op welke wijze de Opdrachtnemer een aanvaardbaar gebruik van door Opdrachtgever eventueel beschikbaar gestelde toegangsmiddelen (pasjes, tokens, e.d.) bewerkstelligt en een sluitende administratie bijhoudt aan de kant van Opdrachtnemer.

- VSP 8.1.SC-12 De Opdrachtnemer dient alle door de Opdrachtgever beschikbaar gestelde toegangsmiddelen (waaronder tokens en pasjes tot objecten, data, ICT en IA) alleen te gebruiken voor het doel waarvoor en onder de voorwaarden waaronder deze zijn verstrekt, waarbij de beveiligingsmaatregelen niet mogen worden omzeild.

3.3.6 Classificatie, beveiliging en opslaglocatie van informatie

<<<<Opdrachtnemer>>>> beschrijft conform richtlijn IBR-1: Beleid voor gegevensclassificatie op welke wijze de beveiliging wordt bewerkstelligd van door Opdrachtgever aangegeven vertrouwelijke documenten, zoals ontwerp, constructietekeningen en datanetwerkschema's.

- VSP 8.2.1 Opdrachtnemer dient aantoonbaar operationeel geborgd te hebben dat alle informatie betrokken bij de Prestatie is geclassificeerd conform IBR-1: *Beleid voor gegevensclassificatie* {10} van Opdrachtgever en dat de hierbij behorende beveiligingsmaatregelen worden nageleefd.
- VSP 8.3.x Opdrachtnemer dient over operationeel geborgde processen te beschikken voor het veilig verwijderen van media, transport van media, en het beheer van verwijderbare media en het onherstelbaar verwijderen van onnodige inhoud van herbruikbare media betrokken bij de Prestatie conform IBR-1 *Beleid voor gegevensclassificatie* {10} van Opdrachtgever.
- VSP 11.2.7 Opdrachtnemer dient aantoonbaar te beschikken over een operationeel geborgd proces voor het vernietigen van data op media bij afvoeren of vervangen van (delen van) informatiesystemen die deze media bevatten en betrokken zijn bij de Prestatie.
- VSP 18.1.CC-09 Gegevens of programmatuur van Opdrachtgever, of door deze gegenereerde metadata, welke zich bevinden op informatiesystemen van Opdrachtnemer, is en blijft ten alle tijden eigendom van Opdrachtgever. Indien gegevens door Opdrachtgever aan Opdrachtnemer zijn verstrekt, mag Personeel dit alleen gebruiken voor het doel waarvoor dit is gebeurd.
- VSP 18.1.CC-10 Opdrachtnemer dient aantoonbaar operationeel geborgde processen te hebben voor het vernietigen van gegevens of programmatuur van Opdrachtgever op apparatuur en alle back-up media van Opdrachtgever, na contractbeëindiging tussen beide partijen.
- VSP 18.1.CC-12 Wanneer gegevens van Opdrachtgever zich bevinden op informatiesystemen van Opdrachtnemer, dient bij contractbeëindiging tussen deze beide partijen, de Opdrachtnemer assistentie te leveren bij de overdracht van deze informatie naar de nieuwe leverancier of terug naar Opdrachtgever.
- VSP 18.1.CC-14 Wanneer gegevens of programmatuur van Opdrachtgever zich bevinden op informatiesystemen van Opdrachtnemer, dient Opdrachtnemer aan te geven waar deze informatiesystemen zich bevinden. Indien deze zich buiten de EU bevinden, mag dit uitsluitend in landen waar een passend niveau van gegevensbescherming wordt geboden; welke landen dit zijn, is bepaald door de Europese Commissie.

3.3.7 Bewustwording, scholing en VOG

<<<<Opdrachtnemer>>>> beschrijft op welke wijze het personeel bewust wordt gemaakt van de Informatiebeveiliging risico's en aantoonbaar over de juiste opleiding, training en vaardigheden beschikt en geheimhouding in acht neemt. Voor de door Opdrachtgever aangegeven doelgroepen dient een Verklaring Omtrent het Gedrag (VOG) te worden opgenomen in de administratie.

- VSP 7.1.1 Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor de screening van het Personeel dat werkzaamheden verricht:
 1. op het gebied van ontwikkelen of herzien van ontwerptekeningen en/of -documenten;

2. ten behoeve van het ontwikkelen, testen, beheren, installeren, configureren en/of bedienen van programmatuur of apparatuur;
 3. in bedienings- of technische ruimtes;
 4. aan kabels en leidingen;
 5. aan beveiligings- en veiligheidsdocumentatie en -instructies,
- betrokken bij de Prestatie middels ten minste een relevante Verklaring Omtrent Gedrag (VOG), waarbij gedurende de contractperiode een screening nooit ouder mag zijn dan 5 jaar. Hangende de aanvraag van een screening kan worden volstaan met een eigen verklaring van betreffende persoon gedurende een periode van maximaal zes weken gerekend vanaf de startdatum van deze persoon bij de Prestatie, welke niet verlengd kan worden.

VSP 7.2.2a Opdrachtnemer dient aantoonbaar operationeel geborgd te hebben dat Personeel een opleiding en -training op het gebied van beveiligingsbewustzijn heeft ontvangen passend bij de aard van de uit te voeren werkzaamheden, alsmede jaarlijkse bijscholing krijgt, waarin ten minste ook persoonlijke verantwoordelijkheid en specifieke beveiligingskaders van Opdrachtgever ter sprake komen.

3.3.8 Fysieke toegang tot werk en technische ruimten en de logische toegang tot informatiesystemen

<<<<Opdrachtnemer>>>> beschrijft op welke wijze de fysieke toegang tot werk en technische ruimten en de logische toegangsbeveiliging tot de informatiesystemen binnen deze ruimten wordt vormgegeven. In de beschrijving staat de wijze waarop de registratie en beheer van de fysieke toegang, de wijze waarop het account en rechtenbeheer alsmede de periodieke controles en schoning van accounts en rechten plaatsvindt. De registraties zijn actueel en kunnen getoetst worden door Opdrachtgever middels Systeemgerichte Contractbeheersing (SCB). In het geval dat Opdrachtgever of een derde partij het fysieke en/of logische toegangsproces regelt, moet Opdrachtnemer toegang via dit proces aanvragen en de spelregels naleven.

- VSP 6.1.2 Opdrachtnemer dient beleid te hebben voor functiescheiding (mits redelijkerwijs mogelijk) bij het beleggen van uitvoerende, controlerende, en beheertaken betrokken bij de Prestatie, en dient dit aantoonbaar operationeel geborgd te hebben in processen, waarmee ook ongeautoriseerde toegang tot bedrijfsmiddelen wordt waargenomen of voorkomen.
- VSE 6.1.2 Informatiesystemen betrokken bij de Prestatie moeten zijn ingericht met een autorisatiemodel en voorzieningen waarmee ongeautoriseerde toegang tot bedrijfsmiddelen wordt waargenomen of voorkomen.
- OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.**
- VSP 9.1.1 Opdrachtnemer dient te zorgen voor een operationeel geborgde procedure voor het verschaffen van fysieke dan wel logische toegang tot informatieverwerkende faciliteiten, inclusief de uitgifte en inname van accounts en autorisaties, en een actuele registratie hiervan.
- VSP 9.1.SC-02 Indien Opdrachtgever of derde partij verantwoordelijk is voor het verschaffen van de fysieke of logische toegang tot informatieverwerkende faciliteiten, dan dient Opdrachtnemer zich te houden aan de door Opdrachtgever of derde partij gehanteerde toegangsprocedure.
- VSE 9.1.2 Informatiesystemen betrokken bij de Prestatie bevatten uitsluitend standaard voor programmatuur noodzakelijke functionele accounts of accounts die zijn aangeleverd door het vigerende autorisatieproces.
- VSP 9.2.x Opdrachtnemer dient minimaal om het halve jaar zowel de fysieke als logische toegangsrechten tot informatieverwerkende faciliteiten van het Personeel te beoordelen en te actualiseren via een operationeel geborgd en formeel proces en zijn medewerking te verlenen voor de periodieke controle en schoning van de eindgebruikers accounts en rechten van Opdrachtgever.
- VSE 9.4.1 Accounts op informatiesystemen betrokken bij de Prestatie beschikken uitsluitend over toegangsrechten gekoppeld aan rollen toegekend via het vigerende autorisatieproces.
- VSE 9.4.2 Informatiesystemen betrokken bij de Prestatie beschikken over een beveiligde inlogprocedure conform de richtlijn IBR-2 *Beleid voor logische toegangsbeveiliging* van Opdrachtgever.
- OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.**
- VSP 11.1.1 Opdrachtnemer dient fysieke beveiligingszones te hebben gedefinieerd en in gebruik te hebben om gebieden te beschermen, die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten, met betrekking tot de Prestatie.
- VSP 11.1.5 Opdrachtnemer dient aantoonbaar operationeel geborgde procedures te hebben voor het werken in beveiligde gebieden, zoals bedoeld in eis VSP 11.1.1.
- VSE 11.1.x Informatieverwerkende faciliteiten betrokken bij de Prestatie zijn fysiek ten minste beveiligd volgens de richtlijn IBR-6 *Richtlijnen voor fysieke beveiliging* van Opdrachtgever.

- VSP 11.2.8 Opdrachtnemer dient aantoonbaar operationeel geborgde procedures te hebben voor de bescherming van onbeheerde informatiesystemen, die betrokken zijn bij de Prestatie.
- VSE 11.2.x Informatiesystemen betrokken bij de Prestatie zijn beschermd tegen verlies, schade, diefstal, compromittering of onderbreking, waarbij ten minste de eisen worden geïmplementeerd uit de richtlijn IBR-6 Richtlijnen voor fysieke beveiliging van Opdrachtgever.

3.3.9 Wachtwoordrichtlijn

<<<<Opdrachtnemer>>>> beschrijft op welke wijze invulling wordt gegeven aan de door Opdrachtgever beschikbaar gestelde wachtwoordrichtlijn. Opdrachtnemer geeft gemotiveerd aan of er afwijkingen bestaan en controleert periodiek de naleving van de wachtwoord-richtlijn door zijn personeel.

- VSP 9.3.1 Opdrachtnemer dient van het Personeel te eisen dat het zich houdt aan de richtlijn IBR-3 *Beleid voor wachtwoordgebruik* {10} van Opdrachtgever bij het gebruiken van authenticatiegegevens gerelateerd aan de Prestatie.
- VSE 9.4.3 Informatiesystemen betrokken bij de Prestatie beschikken over wachtwoordbeheervoorzieningen die het gebruik van sterke wachtwoorden afdwingen die ten minste voldoen aan de richtlijn IBR-3 *Beleid voor wachtwoordgebruik* van Opdrachtgever.
- OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als het standaard beschikken over de functionaliteit de eis te kunnen implementeren.**

3.3.10 Back-up en recovery proces

<<<<Opdrachtnemer>>>> beschrijft het back-up en recovery proces zowel qua proces als de hiervoor gebruikte voorzieningen alsmede de opslag locatie van de back-ups conform de eisen uit de overeenkomst. De Opdrachtnemer test jaarlijks het recovery proces en beschrijft de resultaten ook in het hoofdstuk 8 'Evaluatie en actualisatie van risico's en beheersmaatregelen'.

- VSP 12.3.1a Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het minimaal dagelijks maken van back-ups van alle informatie en programmatuur in gebruik voor de Prestatie.
- VSP 12.3.1b Opdrachtnemer dient het recovery proces dat deel uitmaakt van het back-upproces van alle informatie en programmatuur in gebruik voor de Prestatie, minimaal jaarlijks te testen en naar Opdrachtgever te communiceren over de uitkomst hiervan.
- VSE 12.3.1 Informatiesystemen betrokken bij de Prestatie beschikken over voorzieningen om back-ups te kunnen maken van alle hier op aanwezige informatie en programmatuur. Indien informatiesystemen zich bevinden op de infrastructuur van de Opdrachtgever, moet dit kunnen gebeuren naar de centrale back-up voorziening van de Opdrachtgever.

3.3.11 Beveiliging documentatie technisch beheer en broncode

<<<<Opdrachtnemer>>>> beschrijft op welke wijze de bedien-, beheer en technische documentatie beschermd wordt tegen verlies en ongeautoriseerde kennisname of wijziging.

- VSP 9.4.5 Opdrachtnemer dient aantoonbaar operationeel geborgd te hebben dat uitsluitend Personeel die daartoe specifiek bevoegd is, toegang heeft tot de Broncode van informatiesystemen betrokken bij de Prestatie.
- VSP 12.1.1 Opdrachtnemer dient aantoonbaar operationeel geborgde bedieningsprocedures te hebben en beschikbaar te stellen aan het Personeel en, indien van toepassing de medewerkers van Opdrachtgever, dat ze nodig heeft voor de Prestatie.

3.3.12 Wijzigingsproces, aanpassingen, doorvoeren patches en testen

<<<<Opdrachtnemer>>>> beschrijft hier de inrichting van de OTAP omgeving, het testproces en het wijzigingsproces die gevolgd wordt voor het doorvoeren van (functionele) wijzigingen, updates en patches aan ICT conform de eisen uit de overeenkomst. In voorkomende gevallen dienen security gerelateerde wijzigingen gerapporteerd en specifiek in hoofdstuk 8 'Evaluatie en actualisatie van risico's en beheersmaatregelen' te worden uitgeschreven.

- VSP 7.2.2b Opdrachtnemer dient aantoonbaar operationeel geborgd te hebben dat Personeel verantwoordelijk voor het testen van informatiesystemen betrokken bij de Prestatie, beschikken over actuele en gespecialiseerde kennis, ervaring en opleiding met betrekking tot het testen van de beveiliging hiervan.
- VSP 14.2.SC-06a Opdrachtnemer dient voor informatiesystemen betrokken bij de Prestatie binnen 60 dagen na kennisneming van kwetsbaarheden in het geval van programmatuur en binnen 6 maanden in het geval van apparatuur, kosteloos aanpassingen of patches vrij te geven (ten minste tot de door de Leverancier aangeduide End of Life (EOL) van dit informatiesysteem) met als doel deze kwetsbaarheden te verhelpen.
- 14.2.SC-06b Opdrachtnemer dient te beschikken over een operationeel geborgd proces voor het periodiek doorvoeren van security patches of software updates om de informatiesystemen up to date te houden.
- VSE 12.1.4 Opdrachtnemer dient ontwikkel-, test-, productie- en, indien besteld, educatieve omgevingen aantoonbaar gescheiden (logisch, dan wel fysiek) te hebben voor alle informatiesystemen betrokken bij de Prestatie. Scheiding houdt in dat al het noodzakelijke geregeld moet worden om interferentie tussen de omgevingen te voorkomen en dat de betrouwbaarheid van de productiesystemen gewaarborgd is. De acceptatie- en educatieve omgevingen dienen representatief te zijn voor de productieomgeving, zodanig dat de test- dan wel oefenresultaten het gedrag van de functionaliteit in de productieomgeving weerspiegelen.
- VSE 14.2.9a Informatiesystemen betrokken bij de Prestatie dienen een acceptatietest te hebben ondergaan op alle in dit overeenkomst vermelde systeemeisen voordat deze systemen in productie worden genomen.
- VSE 14.2.9b Informatiesystemen betrokken bij de Prestatie dienen niet in productie genomen te worden voordat alle bevindingen uit de acceptatietest zijn verholpen.
- VSP 14.3.1 Opdrachtnemer dient testgegevens betrokken bij de Prestatie, aantoonbaar zorgvuldig te kiezen, beschermen, controleren, en vernietigen na gebruik.

3.3.13 Beveiliging tegen malware, hardening en patching

<<<<Opdrachtnemer>>>> beschrijft op welke wijze de bescherming tegen malware, het patchproces en hoe het periodiek testen op kwetsbaarheden wordt vormgegeven qua proces en de hiervoor gebruikte voorzieningen alsmede de hardening en patching van ICT en het testen hierop. Hierbij wordt ook het periodiek inventariseren van patchlevels van systemen aangegeven. De resultaten worden beschreven in het Hoofdstuk 8 'Evaluatie en actualisatie van risico's en beheersmaatregelen'. <<<<Opdrachtnemer>>>> beschrijft op welke wijze het patchproces wordt vormgegeven.

- VSP 12.2.1 Opdrachtnemer dient aantoonbaar operationeel geborgde processen te hebben voor bescherming tegen malware op informatiesystemen betrokken bij de Prestatie, waarbij ten minste aandacht wordt besteed aan preventie, detectie, communicatie en herstel.
- VSE 12.2.1 Informatiesystemen betrokken bij de Prestatie zijn voorzien van detectieve en preventieve maatregelen tegen malware.
- VSE 12.2.SC-13 De Opdrachtnemer dient de informatiesystemen betrokken bij de Prestatie te hardenen door:
- Niet noodzakelijke datanetwerkservices uit te zetten;
 - Het verwijderen (patchen) van bekende kwetsbaarheden;
 - Alle poorten die niet nodig zijn te deactiveren/blokkeren;
 - De default account uit te schakelen conform het wachtwoord policy;
 - Indien beschikbaar gebruik te maken van de security opties van de leveranciers;
 - De standaard hardeningsprofielen te volgen voor de gangbare platformen zie hiertoe bijv. de 'Security Benchmarks' van CIS: <http://www.cisecurity.org/>.
- VSP 12.6.SC-16 Opdrachtnemer dient de informatiesystemen betrokken bij de Prestatie te controleren op kwetsbaarheden middels gangbare testmethodieken en conform de BIO Handreiking: Penetratietesten {12} en in afstemming en na goedkeuring door Opdrachtgever de informatiesystemen te patchen.
- VSE 14.2.8a Informatiesystemen betrokken bij de Prestatie zijn aantoonbaar getest op kwetsbaarheden middels gangbare testmethodieken voordat deze in productie worden genomen. In het geval van programmatuur omvat de gehanteerde testmethodiek ten minste de OWASP Top-10 {7}.
- VSE 14.2.8b Alle bekende kwetsbaarheden op informatiesystemen betrokken bij de Prestatie zijn verholpen voordat deze informatiesystemen in productie worden genomen.
- VSP 15.2.1 Opdrachtgever heeft het recht om audit(s) uit te voeren waarin de eisen uit het contract tussen Opdrachtgever en Opdrachtnemer worden getoetst op opzet, bestaan, en/of werking. Aan deze audit dient Opdrachtnemer vrijwillig medewerking te verlenen.

3.3.14 Koppeling van apparatuur

<<<<Opdrachtnemer>>>> beschrijft het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT systemen van RWS en geeft aan op welke wijze de bescherming tegen malware wordt vormgegeven qua proces en voorzieningen bij koppeling van mobiele apparatuur of removable media aan de ICT van Opdrachtgever door Opdrachtnemer of zijn (hulp)personen.

- VSP 9.4.4 Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het controleren van het gebruik van systeemhulpmiddelen, die in staat zijn om beheersmaatregelen te omzeilen voor informatiesystemen betrokken bij de Prestatie. Het gebruik ervan dient gelogd te worden.
- VSP 12.2.SC-17 De Opdrachtnemer dient bij onderhoudswerkzaamheden en koppeling van randapparatuur aan de ICT van de Opdrachtgever de richtlijn IBR-8 *Richtlijn voor het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT systemen van RWS* {10} en Handreiking: BIO Mobile Device Management {9} aan te houden voor bescherming tegen malware.

3.3.15 Logging en monitoring

<<<<Opdrachtnemer>>>> beschrijft op welke wijze logging en monitoring wordt vormgegeven qua proces en voorzieningen in aansluiting op BIO en de richtlijn IBR-6 voor logging van de Opdrachtgever.

De resultaten hiervan worden beschreven in het Hoofdstuk 8 'Evaluatie en actualisatie van risico's en beheersmaatregelen'.

- VSP 12.4.1 Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het voldoende periodiek beoordelen van logbestanden van informatiesystemen betrokken bij de Prestatie, waarbij het interval tussen twee beoordelingen nooit meer mag bedragen dan één maand.
- VSP 12.4.3 Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het maandelijks beoordelen van activiteiten van systeembeheerders en -operators op informatiesystemen betrokken bij de Prestatie, welke zijn vastgelegd in logbestanden.
- VSP 12.4.SC-21 Opdrachtnemer dient logbestanden van informatiesystemen betrokken bij de Prestatie minmaal drie maanden (en bij een vermoed incident minimaal 3 jaar) beschikbaar te houden tenzij met Opdrachtgever een andere bewaartermijn is overeengekomen, en op verzoek deze logbestanden ter inzage te overhandigen aan Opdrachtgever.
- VSE 12.4.x Informatiesystemen betrokken bij de Prestatie leggen gebeurtenissen vast waarbij ten minste wordt voldaan aan de eisen genoemd in de richtlijn IBR-7 *Richtlijnen voor logging* van de Opdrachtgever.
OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.

3.3.16 Datanetwerkkoppelingen

<<<<Opdrachtnemer>>>> geeft een overzicht en beschrijving van alle bestaande datanetwerkkoppelingen (met welke netwerken en partijen, doel van de koppeling en de beveiliging van de datanetwerkkoppeling)

- VSP 13.1.1 Opdrachtnemer dient, om informatie in informatiesystemen te beschermen, aantoonbaar operationeel geborgde processen te hebben voor beheer en beheersing van netwerken betrokken bij de Prestatie, waarbij ten minste aandacht wordt besteed aan onderstaande aspecten:
- Management of network security
 - Technical vulnerability management
 - Identification and authentication
 - Network audit logging and monitoring
 - Intrusion detection and prevention
 - Protection against malicious code
 - Cryptographic based services
 - Business continuity management
- VSE 13.1.3 Groepen van informatiesystemen en gebruikers betrokken bij de Prestatie zijn op basis van functie, rol en/of classificatie in logische of fysieke netwerkdomeinen te scheiden volgens een zoneringsmodel. Voor informatiesystemen geplaatst in de infrastructuur van Opdrachtgever, dient hiervoor het ontwerp (conform PSA) aangehouden te worden van Opdrachtgever.
- VSP 13.1.SC-15 Opdrachtnemer dient zorg te dragen dat het aantal data netwerkkoppelingen beperkt blijft tot alleen de functioneel noodzakelijke, waarbij de koppeling een passende vorm van beveiliging kent en geen onacceptabele risico's oplevert. Voor elke koppeling is een risicoanalyse en afweging gemaakt.
- VSP 13.1.SC-18 Opdrachtnemer dient op verzoek van Opdrachtgever een actueel overzicht aan te leveren waarin alle datanetwerkkoppelingen worden weergegeven met bijbehorende security maatregelen.
- VSE Informatiesystemen betrokken bij de Prestatie die geplaatst gaan worden in de infrastructuur van Opdrachtgever dienen conform de standaard aansluitvoorwaarden {5} van Opdrachtgever ingericht te

- 14.1.SC- zijn.
04a **OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.**
- VSE Informatiesystemen betrokken bij de Prestatie die geplaatst gaan worden in de infrastructuur van Opdrachtgever dienen gebruik te maken van de standaard netwerkdiensten {6} van Opdrachtgever.
- 14.1.SC- **OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.**
04b

3.3.17 Remote Access en gebruik veilige datanetwerkverbindingen en communicatieprotocollen

<<<<Opdrachtnemer>>>> beschrijft indien (beheer)werkzaamheden van de ICT op afstand plaatsvindt en bij uitwisselen van data via alle soorten communicatiefaciliteiten op welke wijze dit vorm krijgt qua proces en (veilige) communicatieprotocollen en of dit geschiedt over beveiligde datanetwerk verbindingen.

Opdrachtnemer dient in het geval van remote acces via de Remote Access oplossing een sluitende administratie erop na te houden over de door Opdrachtgever verstrekte middelen voor toegang (b.v. tokens).

- VSP 6.2.2 Toegang op afstand van alle informatiesystemen betrokken bij de Prestatie in het netwerk van Opdrachtgever is uitsluitend toegestaan via een speciaal hiervoor ingerichte Toegang Derden dienst {2} van Opdrachtgever.
- VSP 13.2.1 Opdrachtnemer dient aantoonbaar operationeel geborgde beleidsregels, procedures en beheersmaatregelen te hebben ter bescherming van het informatietransport betrokken bij de Prestatie, dat via alle soorten communicatiefaciliteiten verloopt.
- VSE 13.2.3 Informatiesystemen betrokken bij de Prestatie die gebruik maken van elektronische berichten met daarin gegevens waarvan de vertrouwelijkheid en/of integriteit moet worden gewaarborgd, dienen hiervoor versleuteling te gebruiken waarbij de gehanteerde onderliggende algoritmes en instellingen uitsluitend de duiding “goed” mogen hebben in de meest actuele versie van het NCSC document Richtlijnen voor Transport Layer Security (TLS) {1}.
OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.
- VSE 14.1.2 Informatiesystemen betrokken bij de Prestatie die informatie uitwisselen via openbare netwerken moeten hiervoor te allen tijde versleutelde protocollen gebruiken waarbij de gehanteerde onderliggende encryptiealgoritmes en instellingen uitsluitend de duiding “goed” mogen hebben in de meest actuele versie van het NCSC document Richtlijnen voor Transport Layer Security (TLS) {1}.
OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.
- VSE 14.1.3 Informatiesystemen betrokken bij de Prestatie en die deel uitmaken van een keten, moeten afhankelijk van de classificatie van de uitgewisselde gegevens, te allen tijde de integriteit dan wel vertrouwelijkheid van deze gegevens waarborgen middels versleuteling, waarbij de gehanteerde onderliggende encryptiealgoritmes en instellingen uitsluitend de duiding “goed” mogen hebben in de meest actuele versie van het NCSC document Richtlijnen voor Transport Layer Security (TLS) {1}.
OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.
- VSE Informatiesystemen betrokken bij de Prestatie zijn voor toegang op afstand en voor beheerdoeleinden niet anders te benaderen dan middels versleutelde protocollen, waarbij de gehanteerde onderliggende encryptiealgoritmes en instellingen uitsluitend de duiding “goed” mogen hebben in de meest actuele versie van het NCSC document Richtlijnen voor Transport Layer Security (TLS) {1}.
14.1.SC-03 **OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.**

3.3.18 (Web-) applicaties en mobiele apps

<<<<Opdrachtnemer>>>> dient te beschrijven hoe de ontwikkeling, onderhoud en beveiliging van de (web-) applicatie en mobile apps vorm krijgt.

- VSE Voor de ontwikkeling en onderhoud van mobiele applicaties dienen minimaal de maatregelen uit de **Handreiking Mobiele App Ontwikkeling en Beheer voor de Rijksoverheid** {4} te worden toegepast.
- 14.1.SC-26 Opdrachtnemer dient gedurende de hele levenscyclus beveiliging integraal onderdeel te maken van het proces voor ontwikkeling en onderhoud van informatiesystemen. Dit dient op basis van een expliciete risicoafweging worden uitgevoerd ten behoeven van het vaststellen van de beveiligingseisen conform de BIO Handreiking: Risicoanalysemethode {11} en de Handreiking: Risicomanagement ISO-27005 {13}. In het geval van programmatuur dienen hiertoe minimaal de maatregelen geïmplementeerd te worden genoemd in het CIP document Grip op SSD - Beveiligingseisen voor (web)applicaties {3}.
- VSP 14.1.1 In de programmatuur die deel uitmaakt van informatiesystemen betrokken bij de Prestatie zijn minimaal de maatregelen geïmplementeerd genoemd in het CIP document *Grip op SSD - Beveiligingseisen voor (web)applicaties* {3}.
- OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.**
- VSP Opdrachtnemer dient gedurende de hele levenscyclus beveiliging integraal onderdeel te maken van het proces voor ontwikkeling en onderhoud van mobiele applicaties, hiertoe dienen minimaal de maatregelen geïmplementeerd te worden genoemd in het document "Handreiking Mobiele App Ontwikkeling en Beheer voor de Rijksoverheid {4}.
- 14.1.SC-24
- VSP 14.2.x Opdrachtnemer dient informatiebeveiliging aantoonbaar operationeel geborgd te hebben in de processen die deel uitmaken van de ontwikkelingslevenscyclus van informatiesystemen betrokken bij de Prestatie, waarbij ten minste de proceseisen worden geïmplementeerd uit de Richtlijn IBR-4 *Richtlijnen voor beveiligen bij ontwikkelen* {10}. In het geval van software dienen hiertoe minimaal de proceseisen worden geïmplementeerd uit het CIP document Grip op SSD - Beveiligingseisen voor (web)applicaties {3}.
- VSP Opdrachtnemer garandeert de werking van informatiesystemen (ten minste tot de door de Leverancier aangeduide End of Life (EOL) hiervan) die onderdeel uitmaken van de Prestatie, op/met producten of programmatuur die niet EOL zijn en met een up-to-date patchniveau, óf biedt een kosteloze upgrade aan om dit alsnog mogelijk te maken.
- 14.2.SC-05

3.3.19 Continuïteit en herstel dienstverlening

<<<<Opdrachtnemer>>>> beschrijft in continuïteitsplannen welke maatregelen zijn getroffen om onderbreking van dienstverlening voor Opdrachtgever tegen te gaan voor de kritieke dienstverleningsprocessen waarmee deze beschermd worden tegen de gevolgen van omvangrijke storingen en herstel bewerkstelligd wordt.

- VSP 17.1.2 Opdrachtnemer dient aantoonbaar te beschikken over een continuïteitsplan voor het handhaven van de Prestatie in ongunstige situaties conform de BIO Algemene handreiking continuïteitsbeheer {14}, waarin ook de continuïteit van de informatiebeveiliging is gewaarborgd.

3.3.20 Testen continuïteitsplannen

<<<<Opdrachtnemer>>>> beschrijft op welke wijze de continuïteitsplannen periodiek worden getest en geactualiseerd. De resultaten worden beschreven in het Hoofdstuk 8 'Evaluatie en actualisatie van risico's en beheersmaatregelen'

- VSP 17.1.3 Opdrachtnemer dient het continuïteitsplan voor de Prestatie minimaal jaarlijks aantoonbaar te verifiëren en bij te werken om te waarborgen dat deze deugdelijk en doeltreffend blijft. Voor het continuïteitsplan kan uitgegaan worden van de BIO Algemene handreiking continuïteitsbeheer {14}.

3.3.21 Beveiliging Spionage

<<<<Opdrachtnemer>>>> beschrijft welke maatregelen er zijn getroffen om documenten, zoals offertes, contracten, netwerkschema's, risicoanalyse, kwetsbaarheidscans en accounts en wachtwoorden te beveiligen tegen spionage in de breedste zin des woords. Indien de Opdrachtnemer ISO27001 gecertificeerd is, dient dit aangetoond te worden door overlegging van het certificaat met het bijbehorende statement of applicability. Dit kan toegevoegd worden aan Hoofdstuk 9 Verklaring Opdrachtnemer.

- VSP 5.1.1 De Opdrachtnemer dient het deel van zijn informatievoorziening dat benodigd is voor de door de Opdrachtgever gevraagde registraties en bestanden en dat benodigd is bij de verwerking van de door de Opdrachtgever geclassificeerde informatie en Documenten, te beveiligen zodanig dat deze zijn beschermd tegen verlies, ongeautoriseerde kennisname en ongeautoriseerde wijziging. Of de Opdrachtnemer is aantoonbaar voor de overeengekomen Prestatie gecertificeerd conform de meest recente versie van de NEN-ISO/IEC 27001 norm of gelijkwaardig, en blijft dit voor ten minste de duur van de Overeenkomst.

- VSP 18.1.3 Opdrachtnemer dient aantoonbaar operationeel geborgde procedures te hebben voor het beschermen tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave, van registraties op informatiesystemen betrokken bij de Prestatie, in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen.
- VSP 18.1.SC-20 De Opdrachtnemer dient maatregelen te treffen om documenten, zoals offertes, contracten, netwerkschema's, risicoanalyse uitwerkingen, kwetsbaarheidscans, penetratie testrapporten en accounts en wachtwoorden te beveiligen tegen spionage in de breedste zin des woords.

3.3.22 Beveiliging van de Informatievoorziening en informatie op mobiele apparatuur

<<<<Opdrachtnemer>>>> beschrijft op welke wijze geclassificeerde informatie en documenten zoals aangegeven door Opdrachtgever zijn beveiligd tegen verlies, ongeautoriseerde kennisname of wijziging bij verwerking in op mobiele apparatuur en kantoor- en netwerkgeving van Opdrachtnemer.

- VSP 6.2.1 Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het beveiligen en versleutelen van gegevens op mobiele apparatuur betrokken bij de Prestatie waarbij rekening wordt gehouden met de richtlijn IBR-1 *Beleid voor gegevensclassificatie* {10}, actualiteit van de veiligheid van de gebruikte versleutelingsmethoden {1} en de Handreiking: BIO Mobile Device Management {9}.
- VSE 6.2.1 Mobiele apparatuur in gebruik door Personeel moet gegevens gerelateerd aan de Prestatie versleuteld opslaan conform richtlijn IBR-1 *Beleid voor gegevensclassificatie* van Opdrachtgever middels cryptografische toepassingen waarbij uitsluitend algoritmes en instellingen worden gebruikt met de duiding "goed" uit de meest actuele versie van het NCSC document Richtlijnen voor Transport Layer Security (TLS) {1}.

3.3.23 Cryptografie

<<<<Opdrachtnemer>>>> beschrijft of en voor welke toepassing cryptografische oplossingen worden ingezet, welke keuzes zijn gemaakt en op welke wijze dit beheerd wordt en hoe het sleutelbeheer is vormgegeven.

- VSP 10.1.x Indien Opdrachtnemer contractueel of wettelijk verplicht is tot de inzet van cryptografie ter bescherming van informatie betrokken bij de Prestatie, dient Opdrachtnemer voor het gebruik van deze cryptografische beheersmaatregelen over beleid en operationeel geborgde processen te beschikken, inclusief het gebruik, de bescherming en de levensduur van de daarbij behorende cryptografische sleutels, tijdens hun gehele levenscyclus conform passende standaarden (bv PKI-Overheid of ISO 11770).
- VSP 18.1.SC-23 De Opdrachtnemer dient bij inzet van certificaten voor publieke webdiensten van RWS of het authenticeren van servers met samenwerkingspartners gebruik te maken van PKI Overheid certificaten die aangevraagd moeten worden bij Opdrachtgever. In overige gevallen dienen de passende standaarden te worden gehanteerd conform de NCSC richtlijn ICT-beveiligingsrichtlijnen voor Transport Layer Security {1}.
- VSE 18.1.5 Informatiesystemen betrokken bij de Prestatie beschermen informatie door middel van cryptografische maatregelen conform relevante overeenkomsten, wet- en regelgeving. Hierbij mogen uitsluitend algoritmes worden toegepast aangeduid als "goed" in de meest actuele versie van het NCSC document *ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)*.
OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als volgt dat het informatiesysteem standaard beschikt over de functionaliteit.

4. Security incidenten, verhoogde dreiging en response

<<<<Opdrachtnemer>>>> beschrijft hier welk proces er is ingericht en wordt gevolgd bij security incidenten (incident response proces) en bij verhoogde dreiging. De status van verhoogde dreiging wordt aangegeven door Opdrachtgever waarop Opdrachtnemer met zijn proces moet aansluiten en binnen de kaders moet handelen zoals aangegeven door Opdrachtgever.

Voor sommige objecten moet Opdrachtgever voldoen aan de meldplicht van ICT-inbreuken. Indien dit aan de orde is zal Opdrachtgever dit kenbaar maken en moet Opdrachtnemer met zijn processen hierop aansluiten.

- VSP 16.1.x Opdrachtnemer dient over een operationeel geborgd proces te beschikken voor de registratie, rapportage en afhandeling van informatiebeveiligingsincidenten die aansluit op het incidentmanagementproces van Opdrachtgever waarbij ten minste de eisen worden geïmplementeerd uit de richtlijn IBR-5 *Richtlijn voor informatiebeveiligingsincidenten* {10}. Ten minste maandelijks dient over deze informatiebeveiligingsincidenten gerapporteerd te worden richting Opdrachtgever.
- VSP De Opdrachtnemer dient over een operationeel geborgd proces te beschikken voor de registratie en de response op security incident en/of event meldingen van het Security Operations Centre van
- 16.1.SC-19 Opdrachtgever.

5. Informatiebeveiliging audit

5.1 Bevindingen

<<<<Opdrachtnemer>>>> beschrijft hier de bevindingen die voortvloeien uit de jaarlijkse audit.

VSP 18.2.1 Opdrachtnemer dient tenminste jaarlijks een audit uit te voeren naar de opzet, bestaan en werking van de maatregelen op het gebied van de informatiebeveiliging gemeld in het contract met Opdrachtgever, en deze Opdrachtgever te rapporteren (als onderdeel van het Informatiebeveiliging Beveiligingsplan IV) over de bevindingen en voorgenomen verbetermaatregelen.

5.2 Risico's van de bevindingen

<<<<Opdrachtnemer>>>> beschrijft hier de risico's in relatie tot de bevindingen uit de voorafgaande paragraaf.

5.3 Aanbevelingen en verbetermaatregelen

<<<<Opdrachtnemer>>>> beschrijft hier de aanbevelingen en de verbetermaatregelen naar aanleiding van de bevinding en hieraan gerelateerde risico's.

6. Evaluatie beveiligingsincidenten en rapportage

6.1 Beveiligingsincidenten

<<<<Opdrachtnemer>>>> beschrijft hier de Informatiebeveiliging beveiligingsincidenten die conform de overeenkomst maandelijks aan Opdrachtgever zijn gerapporteerd langs de door Opdrachtgever aangereikte format en criteria. Een jaaroverzicht wordt door Opdrachtnemer opgesteld om analyse van de incidenten mogelijk te maken.

VSP 16.1.1 Opdrachtnemer dient over een operationeel geborgd proces te beschikken voor de registratie, rapportage en afhandeling van informatiebeveiligingsincidenten die aansluit op het incidentmanagementproces van Opdrachtgever waarbij ten minste de eisen worden geïmplementeerd uit de richtlijn IBR-5 Richtlijn voor informatiebeveiligingsincidenten. Ten minste maandelijks dient over deze informatiebeveiligingsincidenten gerapporteerd te worden richting Opdrachtgever.

6.2 Risico's van beveiligingsincidenten

<<<<Opdrachtnemer>>>> beschrijft hier de analyse resultaten van de Informatiebeveiliging beveiligingsincidenten die beschreven staan in de voorgaande paragraaf.

6.3 Aanbevelingen en verbetermaatregelen

<<<<Opdrachtnemer>>>> beschrijft hier de verbetermaatregelen die reeds zijn getroffen of voortvloeien naar aanleiding van de uitgevoerde analyse uit de voorgaande paragraaf.

7. Evaluatie security gerelateerde wijzigingen

7.1 Security gerelateerde wijzigingen

<<<<Opdrachtnemer>>>> beschrijft hier op welke wijze security gerelateerde wijzigingen worden beoordeeld op mogelijke impact en risico's alvorens de wijziging wordt doorgevoerd.

7.2 Overzicht security gerelateerde wijzigingen

<<<<Opdrachtnemer>>>> beschrijft hier de security gerelateerde wijzigingen die conform de overeenkomst aan Opdrachtgever zijn gerapporteerd langs de door Opdrachtgever aangereikte format en criteria.

7.3 Analyse security gerelateerde wijzigingen en aanbevelingen

<<<<Opdrachtnemer>>>> beschrijft hier de resultaten van de uitgevoerde analyse van de security gerelateerde wijzigingen en geeft aan of er aanbevelingen zijn.

8. Evaluatie en actualisatie van risico's en beheersmaatregelen

8.1 Risicoanalyse en risicoafweging

<<<<Opdrachtnemer>>>> beschrijft hier de resultaten van de door Opdrachtnemer jaarlijks uit te voeren evaluatie en actualisatie in de exploitatiefase. Dit in lijn met de PDCA cyclus en conform de eisen uit de overeenkomst conform de uitgevoerde risicoanalyse en de risicoafweging die is gemaakt.

- VSP 12.6.1 Opdrachtnemer dient voor informatiebeveiliging minimaal jaarlijks een risicoanalyse en risicoafweging conform NEN-ISO/IEC 27005 of gelijkwaardig te maken en passende maatregelen te treffen.
- VSP 18.2.2 Opdrachtnemer dient aantoonbaar operationeel geborgde processen te hebben voor het periodiek beoordelen van de naleving van beleidsregels, normen en andere eisen betreffende beveiliging, bij Personeel betrokken bij de Prestatie.
- VSP 18.2.3 Opdrachtnemer dient aantoonbaar operationeel geborgde processen te hebben voor het periodiek beoordelen van de naleving van technische beleidsregels, normen en andere eisen betreffende beveiliging bij informatiesystemen betrokken bij de Prestatie. Naleving kan aangetoond worden met (geautomatiseerde) kwetsbaarheidsanalyses of pentesten, zie daarvoor de BIO Handreiking: Penetratietesten {12}.

8.2 Testresultaten back-up en recovery proces en continuïteitsplannen en voorzieningen

<<<<Opdrachtnemer>>>> beschrijft hier de resultaten van de jaarlijkse beproevingen van het back-up en recovery proces, de continuïteitsplannen en voorzieningen en geeft aan of er verbeteringen noodzakelijk zijn.

8.3 Informatiebeveiliging beheersmaatregelen

<<<<Opdrachtnemer>>>> beschrijft hier de verbetermaatregelen die voortvloeien uit de door hem periodiek uitgevoerde risicoanalyse en risicoafweging.

8.4 Periodieke rapportage controle accounts en autorisatie

<<<<Opdrachtnemer>>>> rapporteert over de periodieke controle van beheer accounts met bijbehorende autorisaties en de wijze waarop het account en rechtenbeheer is geregeld. Beschrijf ook **hoe periodieke controles en schoning van accounts / rechten plaatsvindt.**

- VSP 9.2.x Opdrachtnemer dient minimaal om het halve jaar zowel de fysieke als logische toegangsrechten tot informatieverwerkende faciliteiten van het Personeel te beoordelen en te actualiseren via een operationeel geborgd en formeel proces en zijn medewerking te verlenen voor de periodieke controle en schoning van de eindgebruikers accounts en rechten van Opdrachtgever.

8.5 Periodieke rapportage pentesten en kwetsbaarheidsscans

<<<<Opdrachtnemer>>>> beschrijft hier de verbetermaatregelen die voortvloeien uit de door hem periodiek uitgevoerde risicoanalyse en risicoafweging naar aanleiding van de uitgevoerde pentesten en kwetsbaarheidsscans.

- VSE 14.2.8a Informatiesystemen betrokken bij de Prestatie zijn aantoonbaar getest op kwetsbaarheden middels gangbare testmethodieken voordat deze in productie worden genomen. In het geval van programmatuur omvat de gehanteerde testmethodiek ten minste de OWASP Top-10 {7}.

8.6 Periodieke rapportage updates patches

<<<<Opdrachtnemer>>>> beschrijft hier alle updates en patches die (nog) niet zijn doorgevoerd en welke updates en patches het afgelopen jaar doorgevoerd zijn.

- VSP 14.2.SC-05 Opdrachtnemer garandeert de werking van informatiesystemen (ten minste tot de door de Leverancier aangeduide End of Life (EOL) hiervan) die onderdeel uitmaken van de Prestatie, op/met producten of programmatuur die niet EOL zijn en met een up-to-date patchniveau, óf biedt een kosteloze upgrade aan om dit alsnog mogelijk te maken.

8.7 Periodieke rapportage statussen explains

<<<<Opdrachtnemer>>>> beschrijft hier de statussen van de bekende explains.

- VSP 18.2.SC-21 Opdrachtnemer dient met Opdrachtgever specifiek af te stemmen voor afwijkingen op de security eisen voor processen en informatiesystemen betrokken bij de Prestatie. Opdrachtnemer dient deze afwijkingen vast te leggen als een explain in het Informatiebeveiliging Beveiligingsplan IV en het eventuele restrisico eveneens te beschrijven.

9. Verklaring Opdrachtnemer

9.1 Certificering

Indien Opdrachtnemer ISO27001 gecertificeerd is, geef de periode van geldigheid van de certificering aan, het certificaat met het bijbehorende statement of applicability wordt als bijlage bijgevoegd.

9.2 Risicoanalyse en risicoafweging

<<<<Opdrachtnemer>>>> geeft hier een samenvatting van de jaarlijkse audit, de resultaten van de analyse van de beveiligingsincidenten, de jaarlijkse risicoanalyse en risicoafweging, de jaarlijkse audit en de evaluatie en actualisatie van het Informatiebeveiliging Beveiligingsplan en de Informatiebeveiliging beheersmaatregelen.

10. Bijlagen

10.1 Relevante bijlagen

<<<<Opdrachtnemer>>>> voegt hier de relevante bijlagen toe met een korte toelichting.

10.2 Explains

Geef de explains aan die van toepassing zijn, welke geldigheidsduur daar bij hoort en welke verbeterplannen hieraan gekoppeld zijn.

Een explain-verklaring bevat:

- De eis waaraan niet wordt voldaan. Voldoende begrijpelijk geformuleerd en reden waarom nog niet kan worden voldaan.
- Risico van de explain
 - Voor de Opdrachtgever
 - Voor andere organisaties (+ verklaring welke organisaties)
 - Welke compenserende maatregelen getroffen worden
 - Beschrijving van het restrisico
- Reden van acceptatie van de explain.
- Geldigheid (duurzaam of tijdelijk met vermelding van einddatum)
- Verantwoordelijke organisatie, actiehouders (=contactpersoon) en lijnmanager
- Refrentienummer en datum van de explain
- Status (kan tussentijds worden bijgehouden).
- Een verwijzing naar een verbeterplan.

11. Begrippenlijst

Cybersecurity

Cybersecurity is het voorkomen van gevaar of schade veroorzaakt door verstoring, uitval of misbruik van ICT en Industriële Automatisering.

Informatievoorziening (IV)

Het geheel aan hulpmiddelen (waaronder ICT en IA), gegevensverzamelingen en organisatorische inrichtingen, dat dient tot het verstrekken van informatie.

Informatie- en Communicatietechnologie (ICT)

Informatie- en Communicatietechnologie omvat een samenhangend geheel van informatiesystemen, hardware en software, operating systemen van servers, de onderliggende technische datanetwerkinfrastructuur met datanetwerken en bijbehorende datanetwerkcomponenten, dataopslag in rekencentrum, computer- en technische ruimten met als doel het mogelijk maken of ondersteunen van de processen.

RWS Infrastructuur

RWS infrastructuur staat voor de netwerkinfrastructuur (het areaal) van RWS: de wegen, vaarwegen en watersystemen.